10/031178

15 T

TRAITE DE COOPERATION EN MATIERE DE BREVETS

PCT

REC'D 03 OCT 2001
WIPO PCT

RAPPORT D'EXAMEN PRELIMINAIRE INTERNATIONAL

(article 36 et règle 70 du PCT)

Référence du dossier du déposant ou du mandataire B-14-310-PCT	**POUR SUITE A DONNER** voir la notification de transmission du rapport d'examen préliminaire international (formulaire PCT/IPEA/416)	
Demande internationale n° PCT/IB00/00847	Date du dépot international *(jour/mois/année)* 23/06/2000	Date de priorité *(jour/mois/année)* 04/08/1999
Classification internationale des brevets (CIB) ou à la fois classification nationale et CIB H04L9/32		
Déposant NAGRAVISION SA et al.		

1. Le présent rapport d'examen préliminaire international, établi par l'administaration chargée de l'examen préliminaire international, est transmis au déposant conformément à l'article 36.

2. Ce RAPPORT comprend 5 feuilles, y compris la présente feuille de couverture.

   ☒ Il est accompagné d'ANNEXES, c'est-à-dire de feuilles de la description, des revendications ou des dessins qui ont été modifiées et qui servent de base au présent rapport ou de feuilles contenant des rectifications faites auprès de l'administration chargée de l'examen préliminaire international (voir la règle 70.16 et l'instruction 607 des Instructions administratives du PCT).

   Ces annexes comprennent 6 feuilles.

3. Le présent rapport contient des indications relatives aux points suivants:

   - I ☒ Base du rapport
   - II ☐ Priorité
   - III ☐ Absence de formulation d'opinion quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle
   - IV ☐ Absence d'unité de l'invention
   - V ☒ Déclaration motivée selon l'article 35(2) quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle; citations et explications à l'appui de cette déclaration
   - VI ☐ Certains documents cités
   - VII ☒ Irrégularités dans la demande internationale
   - VIII ☐ Observations relatives à la demande internationale

Date de présentation de la demande d'examen préliminaire internationale	Date d'achèvement du présent rapport
27/02/2001	01.10.2001
Nom et adresse postale de l'administration chargée de l'examen préliminaire international: Office européen des brevets D-80298 Munich Tél. +49 89 2399 - 0 Tx: 523656 epmu d Fax: +49 89 2399 - 4465	Fonctionnaire autorisé Cretaine, P N° de téléphone +49 89 2399 8828

RAPPORT D'EXAMEN PRÉLIMINAIRE INTERNATIONAL

Demande internationale n° PCT/IB00/00847

I. Base du rapport

1. En ce qui concerne les **éléments** de la demande internationale (*les feuilles de remplacement qui ont été remises à l'office récepteur en réponse à une invitation faite conformément à l'article 14 sont considérées dans le présent rapport comme "initialement déposées" et ne sont pas jointes en annexe au rapport puisqu'elles ne contiennent pas de modifications (règles 70.16 et 70.17)*):

Description, pages:

1-14 version initiale

Revendications, N°:

1-26 reçue(s) le 06/09/2001 avec la lettre du 04/09/2001

Dessins, feuilles:

1/1 version initiale

2. En ce qui concerne la **langue**, tous les éléments indiqués ci-dessus étaient à la disposition de l'administration ou lui ont été remis dans la langue dans laquelle la demande internationale a été déposée, sauf indication contraire donnée sous ce point.

   Ces éléments étaient à la disposition de l'administration ou lui ont été remis dans la langue suivante: , qui est :

   ☐ la langue d'une traduction remise aux fins de la recherche internationale (selon la règle 23.1(b)).

   ☐ la langue de publication de la demande internationale (selon la règle 48.3(b)).

   ☐ la langue de la traduction remise aux fins de l'examen préliminaire internationale (selon la règle 55.2 ou 55.3).

3. En ce qui concerne les **séquences de nucléotides ou d'acide aminés** divulguées dans la demande internationale (le cas échéant), l'examen préliminaire internationale a été effectué sur la base du listage des séquences :

   ☐ contenu dans la demande internationale, sous forme écrite.

   ☐ déposé avec la demande internationale, sous forme déchiffrable par ordinateur.

   ☐ remis ultérieurement à l'administration, sous forme écrite.

   ☐ remis ultérieurement à l'administration, sous forme déchiffrable par ordinateur.

   ☐ La déclaration, selon laquelle le listage des séquences par écrit et fourni ultérieurement ne va pas au-delà de la divulgation faite dans la demande telle que déposée, a été fournie.

   ☐ La déclaration, selon laquelle les informations enregistrées sous déchiffrable par ordinateur sont identiques à celles du listages des séquences Présenté par écrit, a été fournie.

4. Les modifications ont entraîné l'annulation :

☐ de la description, pages :

☒ des revendications, n^{os} : 27-28

☐ des dessins, feuilles :

5. ☐ Le présent rapport a été formulé abstraction faite (de certaines) des modifications, qui ont été considérées comme allant au-delà de l'exposé de l'invention tel qu'il a été déposé, comme il est indiqué ci-après (règle 70.2(c)) :

(Toute feuille de remplacement comportant des modifications de cette nature doit être indiquée au point 1 et annexée au présent rapport)

6. Observations complémentaires, le cas échéant :

V. Déclaration motivée selon l'article 35(2) quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle; citations et explications à l'appui de cette déclaration

1. Déclaration

Nouveauté	Oui :	Revendications	1-26
	Non :	Revendications	
Activité inventive	Oui :	Revendications	1-26
	Non :	Revendications	
Possibilité d'application industrielle	Oui :	Revendications	1-26
	Non :	Revendications	

2. Citations et explications
voir feuille séparée

VII. Irrégularités dans la demande internationale

Les irrégularités suivantes, concernant la forme ou le contenu de la demande internationale, ont été constatées :
voir feuille séparée

Concernant le point V

Déclaration motivée selon l'article 35(2) quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle; citations et explications à l'appui de cette déclaration

L'invention concerne une méthode pour contrôler l'intégrité et l'authenticité d'un ensemble de données, les données étant soit des données reçues dans une unité de décodage de télévision à péage (revendication 1) soit des données mémorisées dans une unité de stockage (revendication 17).

Etat de la technique:

EP-A-0 689 316 (= D4) décrit un module de réception de données sans fil qui reçoit de l'émetteur une signature obtenue par application d'une fonction de Hash sur les données émises et son encryptage. Le module applique la même fonction de Hash et le même cryptage aux données reçues et stockées et compare le résultat avec la signature transmise pour établir l'intégrité des données.

Problème:

Le contrôle d'intégrité étant confié au module récepteur, cette méthode n'est pas adaptée au cas où le récepteur n'est pas fiable pour cette fonction, comme par exemple dans le cas d'un décodeur de télévision à péage recevant des autorisations de décodage des programmes, ces autorisations pouvant être modifiées dans le logiciel du décodeur par l'utilisateur pour augmenter de façon non autorisée son choix de programmes.

Invention:

L'idée de l'invention est de confier les opérations de contrôle d'intégrité des données reçues et stockées dans l'unité de réception/stockage à une unité de sécurité indépendante, réputée inviolable.
Dans la méthode selon la revendication 1, une information de contrôle portant sur les données reçues est élaborée dans le récepteur (par le décodeur ou l'unité de sécurité), cryptée par l'unité de sécurité et envoyée à un centre de gestion par un réseau de

communication. Le centre de gestion décrypte l'information de contrôle et la compare à une valeur de référence, le résultat de la comparaison indiquant l'intégrité ou non étant crypté et envoyé à l'unité de sécurité. Le décodeur seul ne peut donc pas simuler une vérification correcte des données reçues puisqu'il n'a pas accès à la valeur de référence de l'information de contrôle.
Dans la méthode selon la revendication 17, les données stockées dans une unité de stockage contiennent une information de référence de type fonction de Hash cryptée et la comparaison avec l'information de contrôle calculée sur les données stockées est effectuée par l'unité de sécurité indépendante qui possède seule la clé de décryptage. L'unité de stockage ne peut donc pas simuler une vérification correcte des données stockées puisqu'elle n'a pas accès à l'information de référence non cryptée.

Aucun des documents cités dans le rapport de recherche ne divulgue ou suggère le contrôle d'intégrité de données reçues/stockées par une unité de sécurité indépendante de l'unité de réception/stockage. L'objet des revendications indépendantes 1 et 17 implique donc une activité inventive (Article 33 PCT).

Les revendications 2 à 16 et 18 à 26 sont dépendantes et satisfont donc également, en tant que telles, aux conditions requises par le PCT en ce qui concerne la nouveauté et l'activité inventive.

Concernant le point VII
Irrégularités dans la demande internationale

Contrairement à ce qu'exige la règle 5.1 a) ii) PCT, la description n'indique pas l'état de la technique antérieure pertinent exposé dans le document D4 et ne cite pas ce document.

REVENDICATIONS

1. Méthode pour contrôler l'intégrité et l'authenticité d'un ensemble de données reçues (M1 à Mn) dans une unité de décodage de télévision à péage composée d'un décodeur (IRD) et d'une unité de sécurité (SC) ainsi que de moyens de communications (NET, REC) avec un centre de gestion, comprenant les étapes suivantes:
- calculer une information de contrôle (Hx) représentative du résultat d'une fonction dite unidirectionnelle et sans collision, effectuée sur tout ou partie des données (M1 à Mn),

caractérisée en ce qu'elle consiste à:
- transmettre l'information de contrôle (Hx) à l'unité de sécurité et encrypter cette information de contrôle (Hx) par une première clé (k1),
- envoyer au centre de gestion l'information de contrôle k1(Hx) encrypté,
- décrypter par le centre de gestion l'information encryptée de contrôle k1(Hx) et comparer avec une valeur de référence de l'information de contrôle (Hy),
- transmettre des données de gestion (R) incluant le résultat de la comparaison sous forme encryptée à destination de l'unité de sécurité (SC),
- décrypter par l'unité de sécurité (SC), le résultat encrypté de la comparaison et informer l'unité de décodage (IRD) de la validité des données (M1 à Mn).

2. Méthode selon la revendication 1, caractérisée en ce que le centre de gestion renvoie dans les données de gestion (R) la valeur de référence sous forme encryptée k2(Hy) au module de sécurité (SC).

3. Méthode selon les revendications 1 et 2, caractérisée en ce que le calcul est effectué par le décodeur (IRD), le résultat étant transmis à l'unité de sécurité (SC).

4. Méthode selon les revendications 1 à 3, caractérisée en ce que le calcul est effectué par l'unité de sécurité (SC), les données (M1 à Mn) étant transmises du décodeur (IRD) à l'unité de sécurité (SC).

5. Méthode selon les revendications 1 à 4, caractérisée en ce qu'elle consiste à inclure dans les données de gestion (R) un descripteur d'utilisation (D) des données (M1 à Mn), à décrypter les données de gestion (R) et à transmettre le descripteur (D) au décodeur si le résultat de la comparaison est positif, à traiter par le décodeur (IRD) les données (M1 à Mn) selon les directives contenues dans le descripteur (D).

6. Méthode selon les revendications 1 à 5, caractérisée en ce que les données (M1 à Mn) sont accompagnées par une information de validité (CRC, CS, H) desdites données et en ce que le module de sécurité (SC) transmet au décodeur l'information d'utiliser ou non cette information de validité pour contrôler les données (M1 à Mn).

7. Méthode selon la revendication 6, caractérisée en ce que cette information de validité est de type CRC (cyclic redundancy code), CS (checksum) ou Hash (fonction dite unidirectionnelle et sans collision).

8. Méthode selon les revendications 1 à 7, caractérisée en ce qu'elle consiste à inclure dans les données de gestion (R) une information de contrôle global (H'y) représentative du résultat d'une fonction dite unidirectionnelle et sans collision, effectuée sur tout ou partie des données globales (M0 à Mm), ces données étant égales ou englobant les données reçues (M1 à Mn).

9. Méthode selon la revendication 8, caractérisée en ce que les données de gestion (R) comprennent un certificat authentifiant l'émetteur des données (M1 à Mn).

10. Méthode selon la revendication 8, caractérisée en ce qu'elle consiste à calculer périodiquement ou sur requête les valeurs (H'x) représentatives du résultat d'une fonction dite unidirectionnelle et sans collision effectuée sur tout ou partie des données globales (M0 à Mm), l'unité de sécurité (SC) comparant ce résultat (H'x) avec la valeur de référence (H'y).

11. Méthode selon la revendication 10, caractérisée en ce que le calcul est effectué par le décodeur (IRD), le résultat du calcul (H'x) étant transmis à l'unité de sécurité (SC).

12. Méthode selon la revendication 10, caractérisée en ce que le calcul est effectué par l'unité de sécurité (SC), les données (M0 à Mm) étant transmises du décodeur (IRD) à l'unité de sécurité (SC).

13. Méthode selon les revendications 10 à 12, caractérisée en ce que le calcul périodique est effectué sur requête du centre de gestion, de l'unité de sécurité, d'une unité de test (TEST) ou par l'un des moyens de communications (NET, REC).

14. Méthode selon les revendications 10 à 13, caractérisée en ce que le résultat de la comparaison est transmis dans un message d'abonnement usuel au fonctionnement du système.

15. Méthode selon les revendications 10 à 13, caractérisée en ce que la valeur calculée (H'x) est transmise au centre de gestion à l'intérieur de messages d'abonnement usuels au fonctionnement du système, chaque message ne contenant qu'une partie de la valeur calculée (H'x).

16. Méthode selon l'une des revendications précédentes, caractérisée en ce que la transmission au centre de gestion se fait d'une manière différée, selon un horaire défini d'une manière pseudo-aléatoire à l'intérieur de limites prédéfinies.

17. Méthode pour contrôler l'intégrité et l'authenticité d'un ensemble de données mémorisées (M1 à Mn) dans une unité de stockage de données connectée à une unité de sécurité (SC) comprenant les étapes suivantes:

- transmettre de l'unité de stockage à l'unité de sécurité (SC) des données de contrôle (R1) comprenant une information de référence encryptée k1(Hy) représentative du résultat d'une fonction dite unidirectionnelle et sans collision, préalablement effectuée sur tout ou partie des données (M1 à Mn),

- calculer une information de contrôle (Hx) représentative du résultat d'une fonction dite unidirectionnelle et sans collision, effectuée sur tout ou partie des données (M1 à Mn),

- comparer la valeur calculée (Hx) avec la valeur de référence décryptée (Hy) par l'unité de sécurité (SC) et transfert des données de gestion (R2) incluant le résultat de la comparaison à l'unité de stockage.

18. Méthode selon la revendication 17, caractérisée en ce que le calcul est effectué par l'unité de stockage, le résultat du calcul (Hx) étant transmis à l'unité de sécurité (SC).

19. Méthode selon la revendication 17, caractérisée en ce que le calcul est effectué par l'unité de sécurité (SC), les données (M1 à Mn) étant transmises de l'unité de stockage à l'unité de sécurité (SC).

20. Méthode selon les revendications 17 à 19, caractérisée en ce qu'elle consiste à inclure dans les données de contrôle (R1) un descripteur d'utilisation (D) des données (M1 à Mn), et si le résultat de la comparaison est positif, à retourner à l'unité de stockage le descripteur (D) sous forme décryptée, à traiter par l'unité de stockage

les données (M1 à Mn) selon les directives contenues dans le descripteur (D).

21. Méthode selon la revendication 20, caractérisée en ce que les données de contrôle (R1) comprennent un certificat authentifiant l'émetteur des données (M1 à Mn).

22. Méthode selon l'une des revendications 17 à 21, caractérisée en ce qu'elle consiste à calculer périodiquement ou sur requête les valeurs (Hx) représentatives du résultat d'une fonction dite unidirectionnelle et sans collision effectuée sur tout ou partie des données (M1 à Mn), l'unité de sécurité (SC) comparant ce résultat (Hx) avec une valeur de référence (Hy).

23. Méthode selon l'une des revendications 17 à 22, caractérisée en ce qu'elle consiste à :
- stocker les données (M1 à Mn) sous forme encryptées
- transmettre à l'unité de sécurité (SC) dans les données de contrôle (R1) une clé (k3) de décryptage des données (M1 à Mn)
- si le résultat de la comparaison Hx=Hy est positif , à décrypter les données (M1 à Mn) par l'intermédiaire de la clé (k3).

24. Méthode selon la revendication 23, caractérisée en ce que l'opération de décryptage des données (M1 à Mn) est effectuée par l'unité de stockage, la clé de décryptage (k3) étant transmise par l'unité de sécurité (SC).

25. Méthode selon la revendication 23, caractérisée en ce que l'opération de décryptage des données (M1 à Mn) est effectuée par l'unité de sécurité (SC), les données (M1 à Mn) étant transmises de l'unité de stockage à l'unité de sécurité (SC).

26. Méthode selon les revendications 17 à 25, caractérisée en ce qu'elle consiste à inclure dans les données de contrôle (R1) un

descripteur d'utilisation (D) des données (M1 à Mn), à décrypter les données de gestion (R1) et à transmettre le descripteur (D) à l'unité de stockage si le résultat de la comparaison est positif, à traiter par l'unité de stockage les données (M1 à Mn) selon les directives contenues dans le descripteur (D).

This Page Blank (uspto)

(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété Intellectuelle
Bureau international

(43) Date de la publication internationale
15 février 2001 (15.02.2001)

PCT

(10) Numéro de publication internationale
WO 01/11820 A1

(51) Classification internationale des brevets[7]: H04L 9/32, H04N 7/167

(21) Numéro de la demande internationale: PCT/IB00/00847

(22) Date de dépôt international: 23 juin 2000 (23.06.2000)

(25) Langue de dépôt: français

(26) Langue de publication: français

(30) Données relatives à la priorité:
1438/99 4 août 1999 (04.08.1999) CH

(71) Déposant *(pour tous les États désignés sauf US)*: NAGRAVISION SA [CH/CH]; 22, route de Genève, CH-1033 Cheseau-sur-Lausanne (CH).

(72) Inventeurs; et

(75) Inventeurs/Déposants *(pour US seulement)*: HILL, Michael, John [CH/CH]; 10, route de Commugny, CH-1296 Coppet (CH). NICOLAS, Christophe [CH/CH]; 29, rue de Lausanne, CH-1028 Préverenges (CH). SASSELLI, Marco [CH/CH]; 20, chemin des Roches, CH-1803 Chardonne (CH).

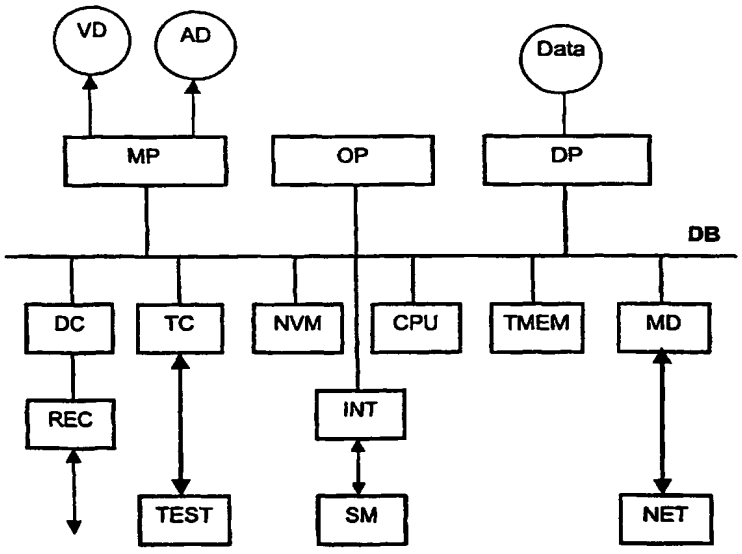
(74) Mandataire: WENGER, Joel; Griffes Consulting S.A., 81, route de Florissant, CH-1206 Genève (CH).

(81) États désignés *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZA, ZW.

[Suite sur la page suivante]

(54) Title: METHOD AND DEVICE FOR GUARANTEEING THE INTEGRITY AND AUTHENTICITY OF A SET OF DATA

(54) Titre: METHODE ET DISPOSITIF POUR GARANTIR L'INTEGRITE ET L'AUTHENTICITE D'UN ENSEMBLE DE DONNEES



(57) Abstract: The invention concerns a method and a device for guaranteeing the integrity and authenticity of data transmitted between a management centre and one or several receiver units, wherein each receiver unit comprises a decoder (IRD) and a security unit (SC) and means for communicating (NET, REC) with the management centre. The method consists in calculating a control information (Hx) representing the result of a function said to be unidirectional and collision-free, performed on all or part of the transmitted data and in transmitting the result to the management centre for verification. The centre will be able to inform the decoder concerning the authenticity of the data by return channels or by the main channel.

[Suite sur la page suivante]

WO 01/11820 A1

(84) **États désignés** *(régional)*: brevet ARIPO (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), brevet eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), brevet européen (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), brevet OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Publiée:

— *Avec rapport de recherche internationale.*

En ce qui concerne les codes à deux lettres et autres abréviations. se référer aux "Notes explicatives relatives aux codes et abréviations" figurant au début de chaque numéro ordinaire de la Gazette du PCT.

(57) Abrégé: Afin de garantir l'intégrité et l'authenticité des données transmises entre un centre de gestion et une ou plusieurs unités réceptrices, chaque unité réceptrice comprend un décodeur (IRD) et une unité de sécurité (SC) ainsi que des moyens de communications (NET, REC) avec le centre de gestion. La méthode consiste à calculer une information de contrôle (Hx) représentative du résultat d'une fonction dite unidirectionnelle et sans collision, effectuée sur tout ou partie de données transmises et de transmettre le résultat au centre de gestion pour vérification. Le centre pourra informer le décodeur de l'authenticité des données par les voies de retour ou par la voie principale.

METHODE ET DISPOSITIF POUR GARANTIR L'INTEGRITE ET L'AUTHENTICITE D'UN ENSEMBLE DE DONNEES

La présente invention est relative au domaine du contrôle d'intégrité et d'authenticité de données, en particulier lors du téléchargement de logiciels.

L'invention s'applique à toute machine comprenant au moins une unité centrale telle que couramment connue et utilisée en informatique, au sens d'un processeur possédant au moins une partie de son programme dans une mémoire à écritures multiples.

Il est connu qu'une altération ou corruption de données laisse des traces dans certaines parties des informations traitées et stockées dans une mémoire, avant ou après traitement. Il est connu d'utiliser une technique mathématique simple telle que le calcul du "checksum" afin de déterminer si les données prises en considération ont été modifiées depuis l'établissement du checksum de référence.

Néanmoins, il se peut que le système de contrôle a été également altéré et qu'il n'est plus en mesure de vérifier le contenu de sa mémoire. Ainsi, il peut y avoir, au cours des opérations mathématiques, propagation d'erreurs aléatoires qui peuvent se compenser, donnant un résultat identique à celui attendu. En conséquence, la vérification par les méthodes connues sera inopérante dans certains cas.

Il y a donc un problème non résolu de façon satisfaisante à ce jour, qui consiste à améliorer la fiabilité et la sécurité procurée par les opérations de vérification connues, en particulier lorsque la même unité est en charge de calculer son checksum et de le comparer à une valeur de référence.

Il est connu, pour rendre visible toute modification des données, d'utiliser une opération unidirectionnelle sur les données c'est-à-dire, une opération qu'il est aisé de réaliser dans un sens mais quasiment impossible dans l'autre. Par

exemple, l'opération x^y est facile à réaliser mais l'opération $\sqrt[y]{x}$ est bien plus difficile.

On entend par opération sans collision une opération selon laquelle aucune combinaison différente des données en entrée ne donne un résultat similaire.

Dans le cadre de l'invention, cette opération unidirectionelle est une application mathématique H d'un ensemble source vers un ensemble objet, dans laquelle chaque élément x de l'ensemble source se voit attribuer une image H(x). Ces fonctions sont particulièrement utiles lorsque ce sont des fonctions dites Hash, telles que définies en page 27 de l'ouvrage RSA Laboratories' Frequently Asked Questions About Today's Cryptography, v4.0. L'élément x peut être d'une longueur quelconque mais H(x) est toujours une suite de caractères de longueur fixe ("fixed-size string"). Une telle fonction est difficile à inverser, c'est-à-dire que la connaissance de H(x) ne permet en général pas de retrouver x. Elle est de plus dite libre de collision lorsqu'elle est injective, c'est-à-dire que H(y)=H(x) entraîne nécessairement y=x, de même que H(y)≠H(x) entraîne nécessairement y≠x.

Le but de l'invention est de s'assurer que les informations contenues dans un décodeur de télévision à péage, sont d'une part, celles que le centre de gestion a transmises et subséquemment, d'autre part, qu'elles n'ont pas été altérées.

Ce but est atteint par une méthode pour contrôler l'intégrité et l'authenticité d'un ensemble de données mémorisées (M1 à Mn) dans une unité de décodage de télévision à péage qui est composée d'un décodeur et d'une unité de sécurité ainsi que de moyens de communications (NET, REC) avec un centre de gestion. Cette méthode consiste à :

- transmettre les données (M1 à Mn) à l'unité de sécurité,
- calculer une information de contrôle (Hx) représentative du résultat d'une fonction dite, unidirectionnelle et sans collision, effectuée sur tout ou partie des données (M1 à Mn),
- encrypter l'information de contrôle (Hx) par une première clé (k1)

- établir la conformité de l'information de contrôle (Hx) par une communication au centre de gestion par l'un des moyens de communications.

Ainsi, l'intégrité des données n'est plus uniquement contrôlée par l'unité de décodage dans laquelle sont contenus ces données mais est assurée par une entité externe, réputée inviolable, l'unité de sécurité.

Selon l'invention, le décodeur peut effectuer lui-même le calcul et transmettre le résultat à l'unité de sécurité ou transmettre les données M1 à Mn à l'unité de sécurité qui effectuera l'opération de calcul de l'information Hash.

Les clés utilisées pour encrypter la communication avec le centre de gestion sont des clés présentes uniquement dans le module de sécurité. Le décodeur n'a pas les moyens pour décrypter ces messages et donc modifier les données transmises par le centre de gestion quand bien même ces messages transitent physiquement par le décodeur.

Ces unités de sécurités sont généralement sous la forme de carte à puce (Smart Card) et comprennent une mémoire, un microprocesseur et des moyens de communications.

Par moyens de communications, on entend soit une liaison bidirectionnelle sur une connexion câblée, soit une sortie par modem, soit une liaison par voie hertzienne. Il est également inclus dans cette expression le media principal véhiculant les données et sur lequel des messages à destination du module sécurité sont acheminés.

L'opération de vérification de la conformité de l'information de contrôle (Hx) peut être exécuté de plusieurs manières.

Le module de sécurité envoie au centre de gestion l'information de contrôle sous forme cryptée, ce dernier étant en charge d'effectuer la vérification. Dans sa réponse, le centre de gestion peut soit envoyer un simple résultat de

comparaison OK/NOK ou renvoyer la valeur de référence. Tous ces messages sont bien entendu encryptés par une clé propre au module de sécurité.

Le centre de gestion mémorise le résultat en référence à chaque unité d'abonné comme preuve soit du bon fonctionnement de l'opération de téléchargement, ou au contraire, de l'altération des données en vue d'une répétition par exemple.

Selon une variante de l'invention, le centre de gestion peut envoyer préalablement la valeur de référence à destination des modules de sécurité. Ainsi, il ne sera pas nécessaire d'appeler le centre de gestion pour la vérification de la conformité de l'information de contrôle calculée Hx.

Dans une autre forme d'exécution, et lors d'une demande de vérification émanant d'une unité de sécurité, le centre de gestion renvoie à titre de résultat de la comparaison, la valeur de référence (Hy) sous forme encryptée k2(Hy) au module de sécurité. De ce fait, le centre de gestion ne se contente pas d'informer l'unité de sécurité si la comparaison est correcte ou pas, mais renvoie la valeur de référence à l'unité de sécurité. Ceci se fera principalement si la comparaison a donné un résultat positif afin que l'unité de sécurité puisse mémoriser la valeur de référence Hy.

Ce renvoi peut être effectué par l'intermédiaire des voies de communications auxiliaires telles que modem, ou par la voie principale des données.

Dans le cas où les données M1 à Mn sont déjà accompagnées par des moyens de vérifications, tels que CRC, Checksum CS ou Hash, l'unité de décodage peut effectuer un premier test grâce à ce moyen connu en soi. Néanmoins, la fiabilité de ce test est à mettre en doute dans le sens que, si les données ont été modifiées par une tierce personne, il est certain que cette personne aura également modifié les moyens de vérifications. C'est pourquoi, selon la méthode de l'invention, l'unité de sécurité peut informer l'unité de décodage de ne pas accepter le résultat du test comme garant de l'authenticité des données mais que cette authenticité soit déterminée selon la méthode décrite plus haut.

Cette variante est importante dans le cas de la mise à jour d'un parc de décodeurs, certains, de l'ancienne génération fonctionnant et donc nécessitant la vérification par Checksum alors que d'autres, ont déjà été équipés par le système selon la méthode revendiquée.

Lorsque l'on télécharge une mise à jour du logiciel, il est d'usage de n'envoyer que la partie ayant subi des modifications. Les données M1 à Mn ne représentant pas l'entier du programme nouvellement mis à jour. C'est pourquoi, afin de conserver un moyen de test fiable sur l'ensemble du programme, il est important de disposer d'une valeur de référence H'y représentative d'une fonction Hash sur le programme nouvellement formé.

Il existe une première méthode qui consiste à établir l'intégrité du programme P0 initial c'est-à-dire avant la mise à jour. Pour cela on dispose du résultat initial H0 de la fonction Hash sur le programme P0 soit initialisé lors de l'installation du programme P0, soit issu de la méthode selon l'invention.

Lorsque l'authenticité des données de la mise à jour a été établie et ces dernières introduites dans la mémoire programme, le module de sécurité peut immédiatement ordonner l'exécution de la fonction Hash sur l'entier du nouveau programme P1 donnant le résultat H1. Ce résultat servira pour les contrôles subséquents ou lors de prochaines mises à jour.

Une variante de cette méthode consiste à obtenir du centre de gestion la nouvelle valeur H'y représentative du résultat de la fonction Hash sur l'entier du nouveau programme P1, ici représenté par M0 à Mm.

Les données de gestion R renvoyée par le centre de gestion peuvent comprendre un descripteur de données D qui indique à l'unité de décodage (IRD) la manière d'utiliser ces données. Ce descripteur peut prendre la forme d'une table contenant les adresses de destinations de données. Ainsi, il n'est pas possible d'utiliser ces données sans ce descripteur, ce dernier étant retourné à l'unité de décodage (IRD) uniquement si la comparaison est positive.

Selon une variante de l'invention, le centre de gestion inclus dans les données de gestion R un certificat permettant d'authentifier l'émetteur des données.

Cette fonction de vérification n'est pas uniquement liée au téléchargement de nouvelles données dans un décodeur mais permet de tester en tout temps la validité et l'authenticité des données. Dans ce cas, l'opération consiste à calculer périodiquement ou sur requête les valeurs (Hx) représentatives du résultat d'une fonction dite unidirectionnelle et sans collision effectuée sur tout ou partie des données (M0 à Mm) en mémoire opérationnelle du décodeur et de transmettre cette information (H'x) à l'unité de sécurité pour comparaison avec une valeur de référence (H'y).

Pour effectuer cette opération, il existe une première méthode qui consiste à ce que le calcul soit effectué par le décodeur, le résultat étant transmis à l'unité de sécurité. Selon une variante de cette méthode, le calcul est effectué par l'unité de sécurité, les données (M0 à Mm) étant transmises du décodeur à l'unité de sécurité (SC).

La requête pour ces opérations de vérifications peut provenir du centre de gestion, de l'unité de sécurité, d'une unité de test ou par l'un des moyens de communications, voire à chaque mise sous tension.

Lorsque l'unité de sécurité compare la valeur calculée H'x à la référence H'y, cette dernière pouvant être représentée soit par la valeur calculée par le décodeur IRD après confirmation de sa validité par le centre de gestion, soit la valeur de référence fournie par le centre de gestion.

Une des manières que certaines personnes mal intentionnées utilisent pour tenter de comprendre le fonctionnement d'un système de télévision à péage, est l'observation des réactions suite à une tentative de modification. C'est pourquoi, l'invention s'étend également sur une méthode de transmission du résultat de la comparaison qui se fait d'une manière différée, par exemple lorsque l'abonné décide d'acheter une émission et qu'un message d'abonnement est envoyé au centre de gestion.

Il est aisé d'inclure dans ce message l'information que les données M1 à Mn ont été altérées. Il sera ainsi difficile de faire le lien entre la modification des données et le blocage du décodeur qui peut intervenir beaucoup plus tard.

Selon une variante, la valeur du résultat du calcul Hx est transmis au centre de gestion. Pour ce faire, et rester discret, le résultat est fractionné et inclus, morceau par morceau dans des messages d'administrations usuels au système.

Le centre de gestion va reconstituer la valeur Hx morceau par morceau et lorsque la valeur est complète, déterminer s'il y a eu des modifications des données.

Un des problèmes rencontré lors de mises à jour d'un grand nombre de décodeurs, est le nombre d'appels au centre de gestion pour obtenir la vérification.

Une solution proposée dans le cadre de cette invention est de répartir d'une manière pseudo-aléatoire les appels au centre de gestion.

Une autre solution précédemment décrite consiste à envoyer la valeur de référence au préalable. Ainsi, si les données sont bien reçues, ce qui constitue la majorité des cas, la mise à jour peut intervenir sans attendre un appel au centre de gestion. Cet appel sera néanmoins effectué pour confirmer que la mise à jour s'est correctement effectuée.

Dans une forme particulière de réalisation, l'ensemble considéré comprend une partie émission, située dans un centre de gestion, et une partie réception qui peut être constituée par un nombre relativement grand d'unités périphériques fonctionnellement semblables. Le but est de garantir que le logiciel envoyé par la partie émission est reçu de manière authentique et intégrale par chacune des unités périphériques. Par analogie avec le vocabulaire de la télévision à péage, qui constitue une application importante mais non exclusive de l'invention, ces unités périphériques seront dans la suite de l'exposé appelées IRD soit Integrated Receiver Decoder comprenant une partie récepteur, un décodeur pour

le traitement du signal reçu par le décodeur, un processeur central ou CPU qui travaille de préférence avec une mémoire non volatile ainsi que divers périphériques.

Une mémoire non volatile est une mémoire dont le contenu est maintenu même lors de la coupure de l'alimentation principale, par exemple au moyen d'une source d'énergie autonome telle que batterie ou pile. D'autres types de mémoires non volatiles peuvent être utilisées, telles que des mémoires dites EEPROM, Flash EPROM ou encore FEPROM. C'est cette mémoire non volatile qui contient les données sauvegardées en cas d'interruption de l'alimentation électrique. Elle est essentielle pour le bon fonctionnement du processeur de l'IRD.

Les informations sont reçues par l'IRD en provenance du centre de gestion, sous forme d'un flux de données arrivant au récepteur de l'unité IRD. Dans le cas de la télévision codée, ou plus généralement interactive, le flux de données comprend des informations vidéo, des informations audio, des informations de données, des applications exécutables telles que des "applets", et enfin des informations de contrôle de données de divers types.

Il s'agit dans ce cas de s'assurer que ces informations sont correctement reçues et interprétées par l'IRD avant leur stockage en mémoire opérationnelle, en particulier les données qui seront exécutées c'est-à-dire le logiciel.

Le récepteur de l'IRD les transmet à un décodeur, qui lui-même les met en circulation dans l'IRD au moyen d'un bus. Sur ce bus sont connectés un processeur spécialisé dans le multimédia, lui-même connecté à un écran de visualisation ainsi qu'à un ou plusieurs haut-parleurs, la mémoire non volatile précitée, et un ou plusieurs sous-ensembles optionnels. C'est le processeur de l'IRD (CPU) qui administre et contrôle le fonctionnement de celui-ci, ainsi que les différents sous-ensembles tels qu'un canal de test, une interface pour carte à puce, une mémoire auxiliaire dite de masse, d'autres processeurs, ou encore un modem. De plus, le centre de gestion peut recevoir des informations en retour,

par exemple par le biais du modem connecté au réseau public de télécommunications.

Ces sous-ensembles peuvent eux-mêmes être la source d'erreurs qu'il s'agit de détecter et de corriger, notamment dans le cas du chargement d'une nouvelle version du logiciel de fonctionnement de l'IRD et particulièrement de son CPU, ou de certains programmes exécutables par l'IRD ou ses composants.

Le logiciel et les données dont l'authenticité et l'intégrité doivent être garanties peuvent être chargés par divers moyens. L'un de ces moyens consiste, comme il a été dit, à utiliser le récepteur précité, en envoyant vers ce récepteur avec le flux de données, et en l'identifiant de manière reconnaissable par l'unité centrale, une mise à jour de mémoire comprenant plusieurs blocs de données M1, M2, ...Mn ainsi qu'une en-tête permettant d'identifier les données M1 à Mn.

Alternativement ou en complément, les blocs de données peuvent parvenir à l'IRD par l'un de ses sous-ensembles optionnels tel le modem par exemple.

Les blocs de données M1, M2, ...Mn peuvent sans inconvénient être envoyés en clair, c'est-à-dire sans encryptage à ce stade, dans le cadre de l'invention.

La méthode selon l'invention consiste, dans cette forme, à appliquer d'abord, au stade de l'émission, une fonction unidirectionnelle ou fonction "hash" à tout ou partie des blocs de données M1, M2, ...Mn pour obtenir un résultat Hx représentatif de l'ensemble M1 à Mn. On peut également traiter les blocs de données M1 à Mn séparément et obtenir le résultat Hx1 correspondant à M1, Hx2 correspondant à M2 ... et Hxn correspondant à Mn. Ce ou ces résultats Hx sont mémorisés par le centre de gestion pour vérification ultérieure.

Un domaine particulièrement crucial pour l'authentification des données concerne les systèmes pour lesquels les données sont transmises par des voies publiques tels que voie hertzienne, téléphonique ou Internet. Dans ce cas, un intrus peut se substituer à un centre de gestion et envoyer des données pour modifier le fonctionnement du système cible.

Il est connu d'adjoindre un cryptogramme lors de la transmission des données pour authentifier ces dernières. Néanmoins ce cryptogramme répond uniquement au besoin d'identifier l'auteur des données mais est sans effet sur un décodeur qui aurait perdu le critère de référence.

La force de la méthode réside d'une part dans la qualité de la fonction unidirectionnelle H et dans la certification de cette signature par une unité de sécurité réputée inviolable. Ainsi, un simple checksum ne permet pas de détecter l'échange de deux blocs de caractères dans les données puisque l'addition est réputée, en mathématiques, commutative et associative. Par contre, un résultat de fonction "hash" Hx est une image très réaliste de x, même si x est beaucoup plus long que Hx. Si des échanges de caractères sont effectués dans la suite de caractères x, la fonction H(x) le détectera immédiatement, et le système ne pourra pas fonctionner suite à cette détection. Il en résulte une sécurité accrue.

Un aspect important de l'invention est de permettre de vérifier à tous moments la validité des données en mémoire dans l'unité périphérique. En effet, la présence dans le module de sécurité de ces informations de contrôle permet au décodeur de procéder à une auto-vérification fiable. Cette vérification donne un résultat sans comparaison avec le checksum habituellement appliqué sur la mémoire programme. Si cette vérification donne un résultat que la référence, l'unité dispose de moyens (liaison modem, liaison sur canal câblé) pour informer une entité extérieure, par exemple le centre de gestion, de la non conformité du programme.

Si le moyen préférentiel de l'invention pour la génération et la transmission des informations de contrôle est le centre de gestion, l'invention recouvre une unité périphérique dont tout ou partie du programme est initialement chargé avec les informations de contrôle telles que décrites ci-dessus. Ceci peut être effectué dans un site de fabrication ou lors de l'initialisation précédant la vente au moyen du processeur, ou par téléchargement de ces informations de contrôle par l'un des périphériques lors d'une étape d'initialisation.

La présente invention est illustrée par le schéma bloc d'un IRD.

Sur cette figure, un IRD ou Integrated Receiver Decoder est représenté, constituant la partie périphérique de l'ensemble auquel est appliqué la méthode selon l'invention dans le mode de réalisation décrit ci-après. Cette IRD comprend un bus central DB sur lequel viennent se connecter tous les différents modules. Le module central de l'IRD est constitué par le processeur CPU qui a pour tâche d'effectuer les différents traitements.

Un récepteur REC reçoit un flux de données comprenant des informations vidéo, audio, des données et des applications exécutables via des supports aussi variés qu'un câble, une antenne hertzienne, une parabole satellite, Internet ou d'autres technologies connues. Ce récepteur REC est relié à une interface DC, elle-même connectée au bus DB.

Sur ce bus DB sont aussi connectés:

- un processeur multimédia MP spécialisé dans le traitement des informations vidéo ou audio, qu'il dirige respectivement vers un écran de visualisation VD et des haut-parleurs AD;
- un canal de test TC, lui-même pouvant être relié à un testeur TEST servant aux réglages d'usine et à la maintenance;
- une mémoire non volatile NVM, rendue indépendante de l'alimentation principale par sa propre source d'alimentation;
- une interface INT pour carte à puce, recevant physiquement une carte à puce SC;
- une mémoire auxiliaire ou encore mémoire de masse TMEM;
- un modem MD, connecté au réseau public NET, celui-ci adoptant des technologies et supports connus;
- d'autres processeurs OP, DP assumant diverses fonctions au gré de l'utilisateur, notamment celles du traitement de données Data.

C'est le CPU qui contrôle les mises à jour de logiciel dont un exemple va être décrit. Il les accepte ou les rejette en fonction du résultat des tests réalisés selon la méthode qui fait l'objet de l'invention.

Ces versions de logiciel du CPU de l'IRD peuvent parvenir à l'IRD par le récepteur REC, par le testeur TEST, par la carte à puce SC, ou encore par le réseau NET. Dans la suite, on décrira plus avant le cas où elles arrivent à l'IRD par le récepteur REC avec le flux d'informations vidéo et audio.

Un ensemble de données, représentant une nouvelle version de logiciel arrivant à l'IRD, est stocké en mémoire temporaire TMEM de l'IRD, avec les informations de service, après avoir été contrôlé quant à son authenticité et son intégrité. Ceci permet au centre de gestion de charger cette version de logiciel dans un grand nombre d'IRD périphériques, et de déclencher sa mise en service sans erreur par l'ensemble de ces IRD.

Une fois que le message contenant les données est reçu par l'IRD, ces données sont décomposée et les différents éléments stockés dans la mémoire temporaire TMEM. L'IRD applique aux blocs de données M1 à Mn le même traitement que lors de l'émission, mais dans l'ordre inverse. Il est clair que dans le cas où l'on reçoit le bloc de données sous forme chiffrée, la première opération consiste à décrypter ces données par la clé publique PuK pour obtenir les données en clair.

L'étape suivante consiste à effectuer la fonction unidirectionnelle H sur les blocs de données M1 à Mn avec pour résultats les valeurs Hy1 à Hyn. Dans le cas où une erreur s'est glissée dans les blocs mémoire M1, M2, ...Mn pendant la transmission du message, cette erreur se répercute sur Hy qui se trouve alors être différent de Hx contenu dans le bloc de contrôle et les données M1 à Mn seront rejetées.

Ces résultats sont transmis à la carte à puce SC qui est en charge de leur authentification. Comme décrit plus haut, cette opération est effectuée grâce à une connexion au centre de gestion, soit immédiatement soit d'une manière différée.

Comme exemple de fonctions H, on connaît les fonctions MD2, MD5 et SHA-1.

Selon une autre variante de l'invention, l'unité contenant les données ne dispose pas de voie de communication avec un centre de gestion. Les données sont livrées à une unité de stockage avec des informations de contrôle (R1) incluant le résultat d'une fonction dite unidirectionnelle et sans collision, dite fonction Hash, effectuée sur tout ou partie des données (M1 à Mn). La particularité de ces données de contrôle (R1) est d'une part qu'elles contiennent le résultat de la fonction Hash pour l'ensemble des données considérées et d'autre part qu'elles sont stockées sous forme encryptée k2(Hy). L'unité de stockage ne peut ni les comprendre, ni les modifier.

Lors de la phase de vérification, l'unité de stockage transmet à l'unité de sécurité ces informations de contrôle sous forme encryptée. L'unité de sécurité dispose des moyens nécessaires pour décrypter ces informations, en particulier pour en extraire le résultat de la fonction Hash (Hy).

De plus, selon une première variante, l'unité de stockage effectue la fonction Hash sur les données M1 à Mn, calcule l'information de contrôle Hx et la transmet à l'unité de sécurité pour comparaison. En retour, l'unité de sécurité envoie des données de retour (R2) à l'unité de stockage incluant le résultat de la comparaison.

A charge ensuite à l'unité de stockage de prendre les mesures nécessaires dans le cas où les données ne sont authentifiées.

Selon une seconde variante, le calcul de l'information de contrôle Hx est effectué par l'unité de sécurité, cette dernière recevant les données M1 à Mn de la part du l'unité de stockage.

Dans une variante donnant une plus grande garantie quant à l'utilisation des données, il est ajouté aux données de contrôle (R1), une clé k3 servant à décrypter les données M1 à Mn.

Ces données sont initialement stockées sous forme encryptée et la fonction Hash se fait sur les données encryptées. Lorsque la vérification de l'intégrité des données est faite par l'unité de sécurité et que le résultat est positif, l'unité de sécurité retourne, dans les données de retour (R2), à l'unité de stockage la clé k3 lui permettant de décrypter les données M1 à Mn.

Selon une variante de la méthode ci-dessus, l'unité de sécurité **ne** retourne pas la clé k3 mais c'est l'unité de stockage qui envoie les données M1 à Mn encryptées à l'unité de sécurité SC pour décryptage.

De la même manière que précédemment, ce contrôle peut être effectué à tout moment durant le fonctionnement de l'unité de stockage.

Les données de contrôle (R1) comprennent un descripteur de données D qui indique à l'unité de stockage la manière d'utiliser ces données. Ce descripteur peut prendre la forme d'une table contenant les adresses de destinations de données. Ainsi, il n'est pas possible d'utiliser ces données sans ce descripteur, ce dernier étant retourné à l'unité de stockage uniquement si la comparaison est positive.

Il est également prévu d'adjoindre au données de contrôle (R1) un certificat authentifiant l'émetteur de données, et ceci afin de conserver une trace dans l'unité de sécurité.

REVENDICATIONS

1. Méthode pour contrôler l'intégrité et l'authenticité d'un ensemble de données reçues (M1 à Mn) dans une unité de décodage de télévision à péage composée d'un décodeur (IRD) et d'une unité de sécurité (SC) ainsi que de moyens de communications (NET, REC) avec un centre de gestion, comprenant les étapes suivantes:

- calculer une information de contrôle (Hx) représentative du résultat d'une fonction dite unidirectionnelle et sans collision, effectuée sur tout ou partie des données (M1 à Mn),
- encrypter l'information de contrôle (Hx) par une première clé (k1) par l'unité de sécurité
- établir la conformité de l'information de contrôle (Hx) par des données de gestion (R) provenant du centre de gestion par l'un des moyens de communications.

2. Méthode selon la revendication 1, caractérisée en ce que l'établissement de la conformité est effectué par comparaison avec une valeur de référence (Hy) reçue de la part du centre de gestion.

3. Méthode selon la revendication 1, caractérisée en ce que l'établissement de la conformité comprend les étapes suivantes:

- envoyer au centre de gestion l'information de contrôle k1(Hx) encrypté,
- décrypter par le centre de gestion l'information encryptée de contrôle k1(Hx) et comparer avec une valeur de référence de l'information de contrôle (Hy),
- transmettre des données de gestion (R) incluant le résultat de la comparaison sous forme encryptée à destination de l'unité de sécurité (SC),
- décrypter par l'unité de sécurité (SC), le résultat encrypté de la comparaison et informer l'unité de décodage (IRD) de la validité des données (M1 à Mn).

4. Méthode selon la revendication 3, caractérisée en ce que le centre de gestion renvoie dans les données de gestion (R) la valeur de référence sous forme encryptée k2(Hy) au module de sécurité (SC).

5. Méthode selon les revendications 1 à 4, caractérisée en ce que le calcul est effectué par le décodeur (IRD), le résultat étant transmis à l'unité de sécurité (SC).

6. Méthode selon les revendications 1 à 4, caractérisée en ce que le calcul est effectué par l'unité de sécurité (SC), les données (M1 à Mn) étant transmises du décodeur (IRD) à l'unité de sécurité (SC).

7. Méthode selon les revendications 3 à 6, caractérisée en ce qu'elle consiste à inclure dans les données de gestion (R) un descripteur d'utilisation (D) des données (M1 à Mn), à décrypter les données de gestion (R) et à transmettre le descripteur (D) au décodeur si le résultat de la comparaison est positif, à traiter par le décodeur (IRD) les données (M1 à Mn) selon les directives contenues dans le descripteur (D).

8. Méthode selon les revendications 1 à 7, caractérisée en ce que les données (M1 à Mn) sont accompagnées par une information de validité (CRC, CS, H) desdites données et en ce que le module de sécurité (SC) transmet au décodeur l'information d'utiliser ou non cette information de validité pour contrôler les données (M1 à Mn).

9. Méthode selon la revendication 8, caractérisée en ce que cette information de validité est de type CRC (cyclic redundancy code), CS (checksum) ou Hash (fonction dite unidirectionnelle et sans collision).

10. Méthode selon les revendications 1 à 9, caractérisée en ce qu'elle consiste à inclure dans les données de gestion (R) une information de contrôle global (H'y) représentative du résultat d'une fonction dite unidirectionnelle et sans collision, effectuée sur tout ou partie des données globales (M0 à Mm), ces données étant égales ou englobant les données reçues (M1 à Mn).

11. Méthode selon la revendication 10, caractérisée en ce que les données de gestion (R) comprennent un certificat authentifiant l'émetteur des données (M1 à Mn).

12. Méthode selon la revendication 10, caractérisée en ce qu'elle consiste à calculer périodiquement ou sur requête les valeurs (H'x) représentatives du résultat d'une fonction dite unidirectionnelle et sans collision effectuée sur tout ou partie des données globales (M0 à Mm), l'unité de sécurité (SC) comparant ce résultat (H'x) avec la valeur de référence (H'y).

13. Méthode selon la revendication 12, caractérisée en ce que le calcul est effectué par le décodeur (IRD), le résultat du calcul (H'x) étant transmis à l'unité de sécurité (SC).

14. Méthode selon la revendication 12, caractérisée en ce que le calcul est effectué par l'unité de sécurité (SC), les données (M0 à Mm) étant transmises du décodeur (IRD) à l'unité de sécurité (SC).

15. Méthode selon les revendications 12 à 14, caractérisée en ce que le calcul périodique est effectué sur requête du centre de gestion, de l'unité de sécurité, d'une unité de test (TEST) ou par l'un des moyens de communications (NET, REC).

16. Méthode selon les revendications 12 à 15, caractérisée en ce que le résultat de la comparaison est transmis dans un message d'abonnement usuel au fonctionnement du système.

17. Méthode selon les revendications 12 à 15, caractérisée en ce que la valeur calculée (H'x) est transmise au centre de gestion à l'intérieur de messages d'abonnement usuels au fonctionnement du système, chaque message ne contenant qu'une partie de la valeur calculée (H'x).

18. Méthode selon l'une des revendications précédentes, caractérisée en ce que la transmission au centre de gestion se fait d'une manière différée, selon un horaire défini d'une manière pseudo-aléatoire à l'intérieur de limites prédéfinies.

19. Méthode pour contrôler l'intégrité et l'authenticité d'un ensemble de données mémorisées (M1 à Mn) dans une unité de stockage de données connectée à une unité de sécurité (SC) comprenant les étapes suivantes:

- transmettre de l'unité de stockage à l'unité de sécurité (SC) des données de contrôle (R1) comprenant une information de référence encryptée k1(Hy) représentative du résultat d'une fonction dite unidirectionnelle et sans collision, effectuée sur tout ou partie des données (M1 à Mn),

- calculer une information de contrôle (Hx) représentative du résultat d'une fonction dite unidirectionnelle et sans collision, effectuée sur tout ou partie des données (M1 à Mn),

- comparer la valeur calculée (Hx) avec la valeur de référence décryptée (Hy) par l'unité de sécurité (SC) et transfert des données de gestion (R2) incluant le résultat de la comparaison à l'unité de stockage.

20. Méthode selon la revendication 19, caractérisée en ce que le calcul est effectué par l'unité de stockage, le résultat du calcul (Hx) étant transmis à l'unité de sécurité (SC).

21. Méthode selon la revendication 19, caractérisée en ce que le calcul est effectué par l'unité de sécurité (SC), les données (M1 à Mn) étant transmises de l'unité de stockage à l'unité de sécurité (SC).

22. Méthode selon les revendications 19 à 21, caractérisée en ce qu'elle consiste à inclure dans les données de contrôle (R1) un descripteur d'utilisation (D) des données (M1 à Mn), et si le résultat de la comparaison est positif, à retourner à l'unité de stockage le descripteur (D) sous forme décryptée, à traiter par l'unité de stockage les données (M1 à Mn) selon les directives contenues dans le descripteur (D).

23. Méthode selon la revendication 22, caractérisée en ce que les données de contrôle (R1) comprennent un certificat authentifiant l'émetteur des données (M1 à Mn).

24. Méthode selon l'une des revendications 19 à 23, caractérisée en ce qu'elle consiste à calculer périodiquement ou sur requête les valeurs (Hx) représentatives du résultat d'une fonction dite unidirectionnelle et sans collision effectuée sur tout ou partie des données (M1 à Mn), l'unité de sécurité (SC) comparant ce résultat (Hx) avec une valeur de référence (Hy).

25. Méthode selon l'une des revendications 19 à 24, caractérisée en ce qu'elle consiste à :
- stocker les données (M1 à Mn) sous forme encryptées
- transmettre à l'unité de sécurité (SC) dans les données de contrôle (R1) une clé (k3) de décryptage des données (M1 à Mn)
- si le résultat de la comparaison Hx=Hy est positif , à décrypter les données (M1 à Mn) par l'intermédiaire de la clé (k3).

26. Méthode selon la revendication 25, caractérisée en ce que l'opération de décryptage des données (M1 à Mn) est effectuée par l'unité de stockage, la clé de décryptage (k3) étant transmise par l'unité de sécurité (SC).

27. Méthode selon la revendication 25, caractérisée en ce que l'opération de décryptage des données (M1 à Mn) est effectuée par l'unité de sécurité (SC), les données (M1 à Mn) étant transmises de l'unité de stockage à l'unité de sécurité (SC).

28. Méthode selon les revendications 19 à 27, caractérisée en ce qu'elle consiste à inclure dans les données de contrôle (R1) un descripteur d'utilisation (D) des données (M1 à Mn), à décrypter les données de gestion (R1) et à transmettre le descripteur (D) à l'unité de stockage si le résultat de la comparaison est positif, à traiter par l'unité de stockage les données (M1 à Mn) selon les directives contenues dans le descripteur (D).

This Page Blank (uspto)

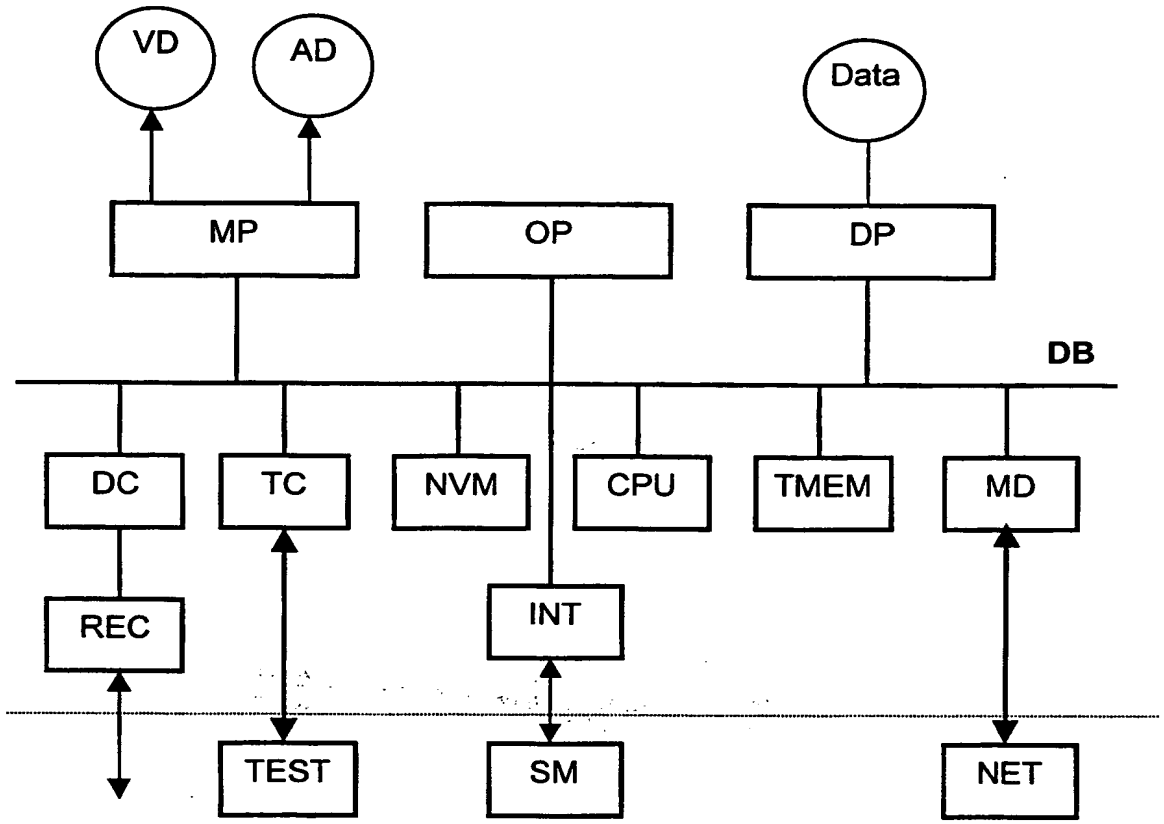


Fig. 1

This Page Blank (uspto)

INTERNATIONAL SEARCH REPORT

International Application No
PCT/IB 00/00847

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L9/32 H04N7/167

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L H04N

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal, WPI Data, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EP 0 752 786 A (THOMSON CONSUMER ELECTRONICS) 8 January 1997 (1997-01-08) abstract page 2, line 22 - line 30 page 3, line 41 - line 58 page 6, line 43 -page 7, line 2 page 7, line 45 - line 59 page 9, line 7 - line 13 page 11, line 19 - last line claims 1-3 figure 9	1,2,19
A	EP 0 723 371 A (THOMSON MULTIMEDIA SA) 24 July 1996 (1996-07-24) column 4, line 55 -column 5, line 28	1,2,19

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
19 October 2000	25/10/2000

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Holper, G

Form PCT/ISA/210 (second sheet) (July 1992)

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
A	WO 99 07150 A (SCIENTIFIC ATLANTA) 11 February 1999 (1999-02-11) page 56, line 1 - line 4 page 73, line 9 - line 23 page 74, line 20 - line 27	1,2,19
A	EP 0 689 316 A (AT & T CORP) 27 December 1995 (1995-12-27) abstract column 1, line 55 -column 2, line 28 column 4, line 45 -column 5, line 46 column 7, line 8 -column 8, line 3 claim 1 figures 1,3	1

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/IB 00/00847

Patent document cited in search report		Publication date	Patent family member(s)		Publication date
EP 0752786	A	08-01-1997	US	5625693 A	29-04-1997
			BR	9602980 A	06-01-1998
			CN	1146122 A	26-03-1997
			DE	69606673 D	23-03-2000
			DE	69606673 T	06-07-2000
			ES	2143111 T	01-05-2000
			JP	9121340 A	06-05-1997
			TR	970038 A	21-01-1997
EP 0723371	A	24-07-1996	FR	2729521 A	19-07-1996
			JP	8307850 A	22-11-1996
WO 9907150	A	11-02-1999	AU	1581699 A	08-03-1999
			AU	8670598 A	22-02-1999
			AU	8679798 A	22-02-1999
			AU	8679898 A	22-02-1999
			AU	8764298 A	22-02-1999
			AU	8823398 A	22-02-1999
			AU	8823698 A	22-02-1999
			EP	1010323 A	21-06-2000
			EP	1010324 A	21-06-2000
			EP	1010325 A	21-06-2000
			EP	1013091 A	28-06-2000
			EP	1000508 A	17-05-2000
			EP	1000509 A	17-05-2000
			EP	1000511 A	17-05-2000
			WO	9907145 A	11-02-1999
			WO	9907146 A	11-02-1999
			WO	9907147 A	11-02-1999
			WO	9907148 A	11-02-1999
			WO	9907149 A	11-02-1999
			WO	9909743 A	25-02-1999
			US	6105134 A	15-08-2000
EP 0689316	A	27-12-1995	CA	2149067 A	23-12-1995
			JP	8032575 A	02-02-1996

This Page Blank (uspto)

RAPPORT DE RECHERCHE INTERNATIONALE

de internationale No
PCT/IB 00/00847

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
CIB 7 H04L9/32 H04N7/167

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
CIB 7 H04L H04N

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si réalisable, termes de recherche utilisés)
EPO-Internal, WPI Data, INSPEC

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	EP 0 752 786 A (THOMSON CONSUMER ELECTRONICS) 8 janvier 1997 (1997-01-08) abrégé page 2, ligne 22 - ligne 30 page 3, ligne 41 - ligne 58 page 6, ligne 43 -page 7, ligne 2 page 7, ligne 45 - ligne 59 page 9, ligne 7 - ligne 13 page 11, ligne 19 - dernière ligne revendications 1-3 figure 9 ---	1,2,19
A	EP 0 723 371 A (THOMSON MULTIMEDIA SA) 24 juillet 1996 (1996-07-24) colonne 4, ligne 55 -colonne 5, ligne 28 --- -/--	1,2,19

[X] Voir la suite du cadre C pour la fin de la liste des documents

[X] Les documents de familles de brevets sont indiqués en annexe

° Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent

"E" document antérieur, mais publié à la date de dépôt international ou après cette date

"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)

"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens

"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

"X" document particulièrement pertinent; l'inven tion revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

"Y" document particulièrement pertinent; l'inven tion revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée	Date d'expédition du présent rapport de recherche internationale
19 octobre 2000	25/10/2000

Nom et adresse postale de l'administration chargée de la recherche internationale	Fonctionnaire autorisé
Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Holper, G

1

Formulaire PCT/ISA/210 (deuxième feuille) (juillet 1992)

C.(suite) DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec, le cas échéant, l'indicationdes passages pertinents	no. des revendications visées
A	WO 99 07150 A (SCIENTIFIC ATLANTA) 11 février 1999 (1999-02-11) page 56, ligne 1 - ligne 4 page 73, ligne 9 - ligne 23 page 74, ligne 20 - ligne 27	1,2,19
A	EP 0 689 316 A (AT & T CORP) 27 décembre 1995 (1995-12-27) abrégé colonne 1, ligne 55 -colonne 2, ligne 28 colonne 4, ligne 45 -colonne 5, ligne 46 colonne 7, ligne 8 -colonne 8, ligne 3 revendication 1 figures 1,3	1

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

de internationale No
PCT/IB 00/00847

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
EP 0752786 A	08-01-1997	US 5625693 A	29-04-1997
		BR 9602980 A	06-01-1998
		CN 1146122 A	26-03-1997
		DE 69606673 D	23-03-2000
		DE 69606673 T	06-07-2000
		ES 2143111 T	01-05-2000
		JP 9121340 A	06-05-1997
		TR 970038 A	21-01-1997
EP 0723371 A	24-07-1996	FR 2729521 A	19-07-1996
		JP 8307850 A	22-11-1996
WO 9907150 A	11-02-1999	AU 1581699 A	08-03-1999
		AU 8670598 A	22-02-1999
		AU 8679798 A	22-02-1999
		AU 8679898 A	22-02-1999
		AU 8764298 A	22-02-1999
		AU 8823398 A	22-02-1999
		AU 8823698 A	22-02-1999
		EP 1010323 A	21-06-2000
		EP 1010324 A	21-06-2000
		EP 1010325 A	21-06-2000
		EP 1013091 A	28-06-2000
		EP 1000508 A	17-05-2000
		EP 1000509 A	17-05-2000
		EP 1000511 A	17-05-2000
		WO 9907145 A	11-02-1999
		WO 9907146 A	11-02-1999
		WO 9907147 A	11-02-1999
		WO 9907148 A	11-02-1999
		WO 9907149 A	11-02-1999
		WO 9909743 A	25-02-1999
		US 6105134 A	15-08-2000
EP 0689316 A	27-12-1995	CA 2149067 A	23-12-1995
		JP 8032575 A	02-02-1996

This Page Blank (uspto)